

SecuraLive® ULTIMATE SECURITY

Home Edition for Windows

USER GUIDE



SECURALIVE®

SECURE AND PROTECT

SecuraLive® ULTIMATE SECURITY

USER MANUAL

Introduction:

Welcome to SecuraLive® Ultimate Security Home Edition.

SecuraLive® Ultimate Security is a collection of high end technologies that work in perfect synergy, having one common goal: to protect your system & network and valuable data against computer viruses. It represents a superior solution for any Windows PC.

SecuraLive® Ultimate Security incorporates Ultimate Security, Antispyware, Anti Malware & Antiroot kit technology. With firewall & sophisticated protection capabilities Ultimate Security ensures that your valuable data and programs are always protected.

This manual describes the SecuraLive® Ultimate Security installation and operation. For further options and information, please visit our website:

www.securalive.com

Your SecuraLive® Team.

INSTALLATION

BEFORE STARTING INSTALLATION

- Make sure that no other virus protection solutions are installed on the system.
- The automatic protection functions of various security solutions may interfere with each other.
- Establish an Internet connection for downloading the setup.

INSTALL

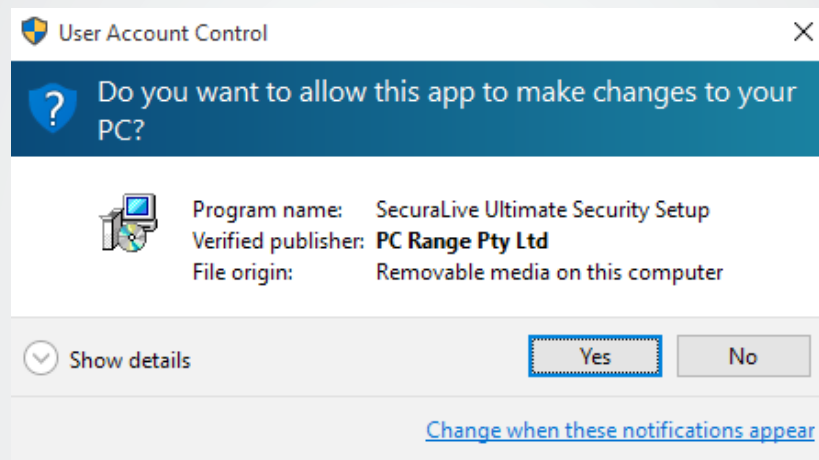
The installation program runs in a self-explanatory dialog mode. Every Windows contains a certain selection of buttons to control the installation process.

The most important buttons are assigned the following functions.

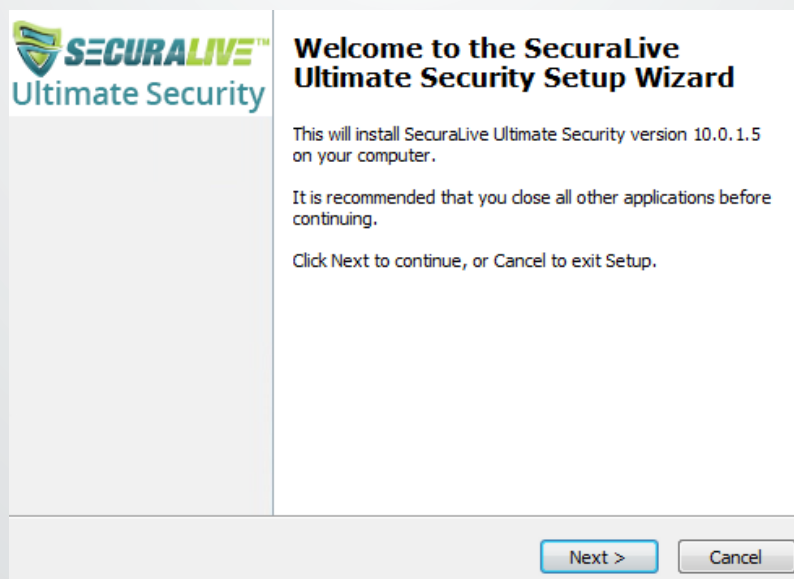
Go to next step	NEXT
Go to previous step	BACK
To process installation	INSTALL
Action finished	FINISH

INSTALLING YOUR SECURALIVE ULTIMATE SECURITY PROGRAM

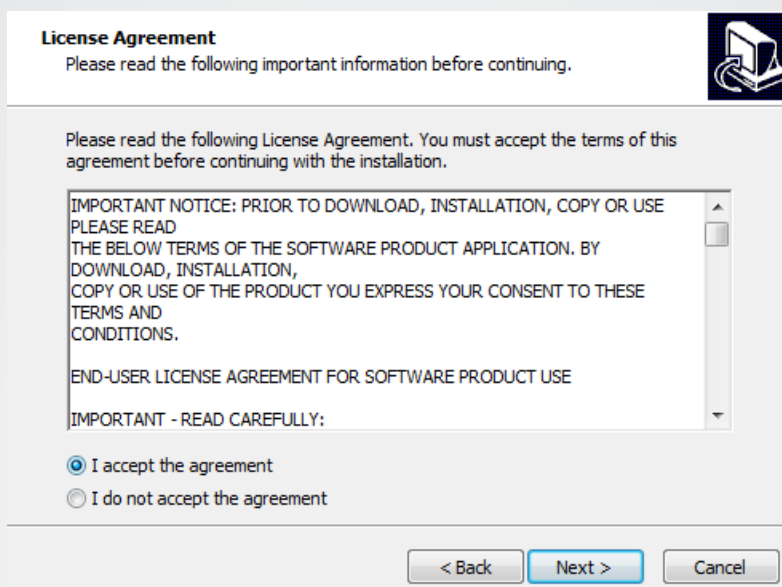
- Install by running the “SecuraLiveUS.exe” installation file by double clicking on it.
- Clicking “Yes” will take you to the SecuraLive® Ultimate Security Setup screen:



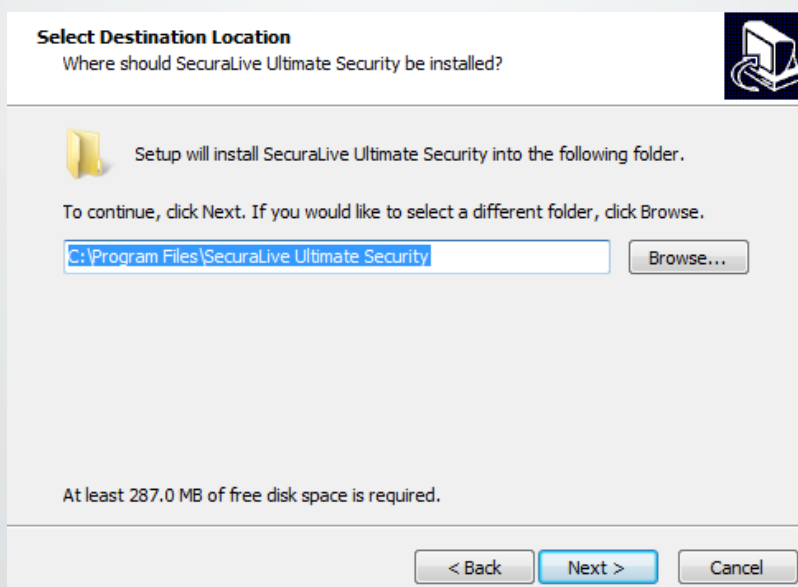
- Click “Next” and the installation Wizard will then guide you through the rest of the installation process.



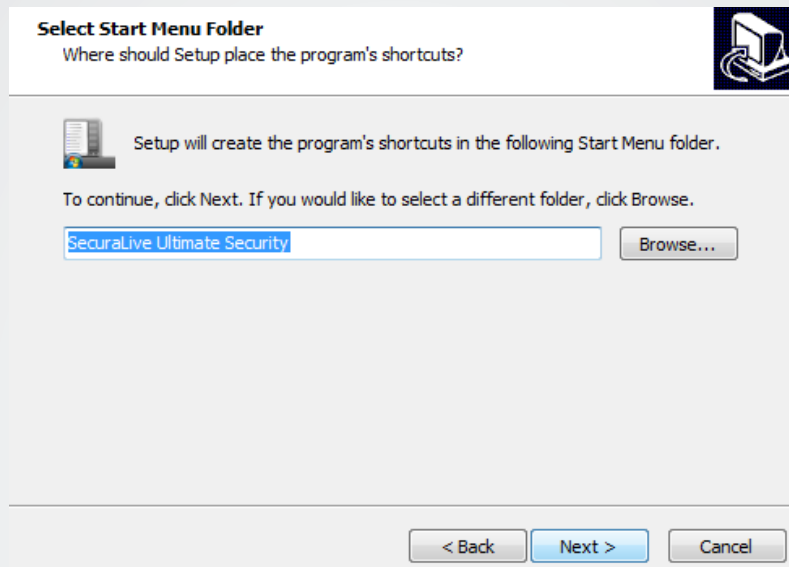
- First you will be asked to read about the minimum system requirements and then confirm that you agree to the end-user license conditions.
- To continue, click on “I accept the agreement”, this enables “Next” for further steps.



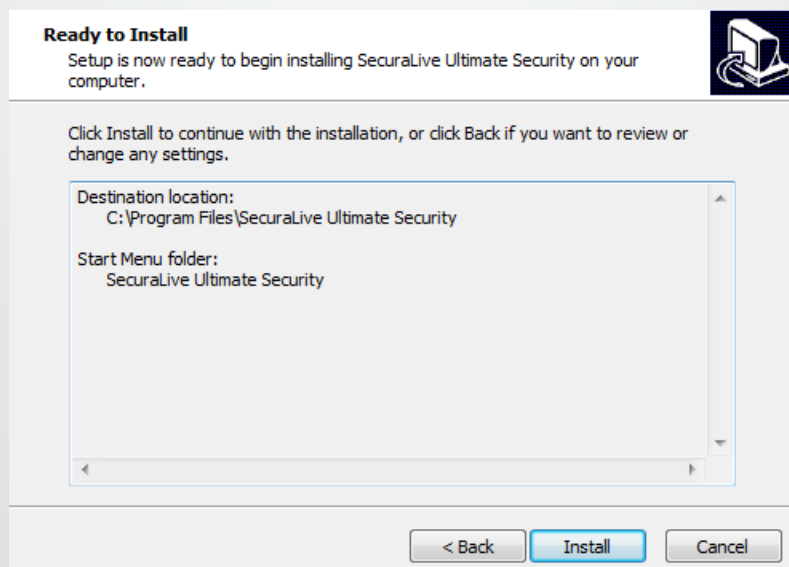
- Clicking on “Next” will navigate you to the destination selection Windows.
- You will be asked to confirm the destination directory, i.e. where the program files will be saved. The program will select this automatically or will create a new directory if it doesn't already exist. It is recommended to accept the default destination directory and simply click on “Next” to continue.



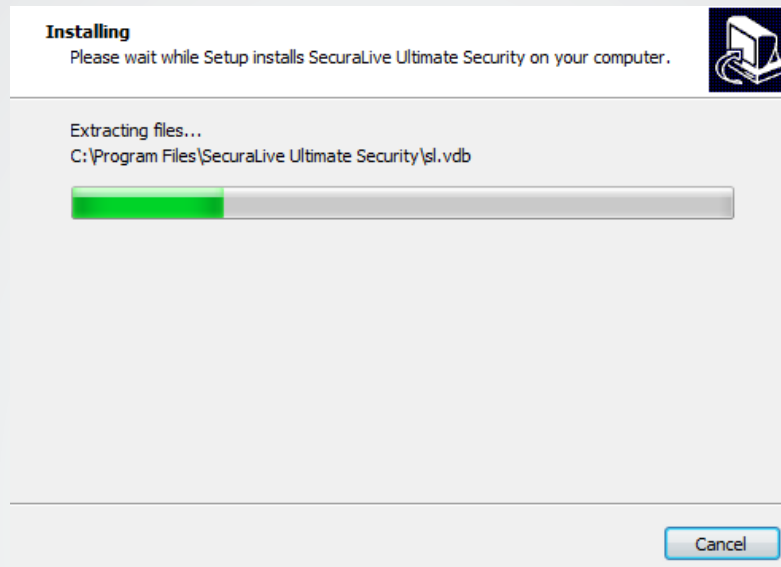
- It will take you to the “Select Start Menu folder” Windows to place the program’s shortcuts. By default it will store in the “SecuraLive[®] Ultimate Security” folder, otherwise you can browse a different location. Click on “Next” to continue.



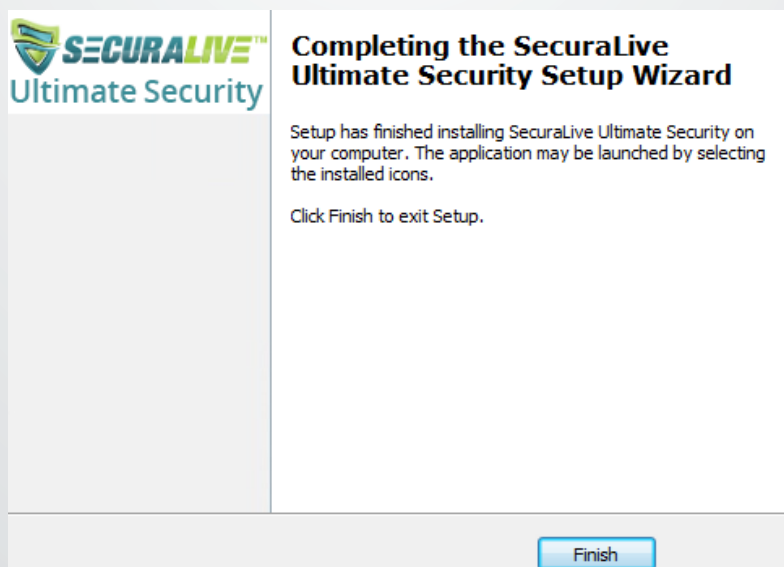
- Now the setup is ready to install the SecuraLive[®] Ultimate Security. Click on “Install” for the installation process.



- The installation progress will display a green progression bar as shown in the screen below.



- The complete green colored bar confirms that installation has been successfully completed and ensures you with the “Finish” setup wizard.
- Click on “Finish” to complete the process. With this the installation task has been completed.



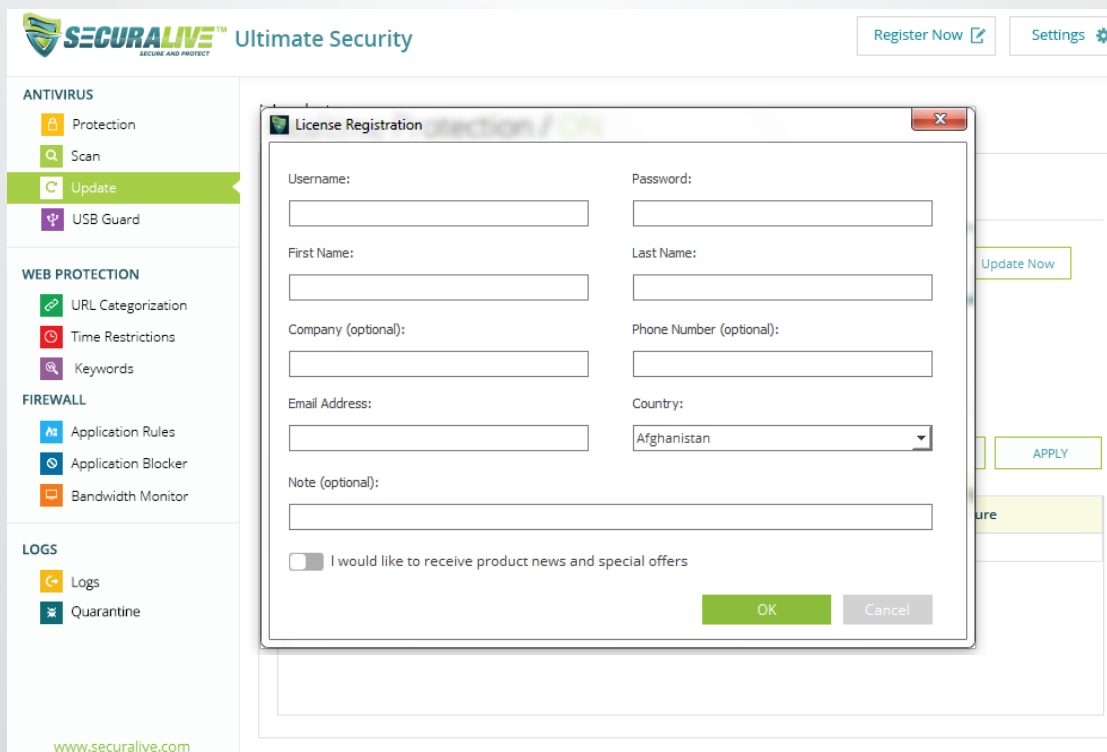
Registering SecuraLive® Ultimate Security:

Please Note:

You are not required to register your trial version of SecuraLive® Ultimate Security. Below Registration process is only applicable if you have already purchased the premium license.

- Please click on Register Now button on the top right hand corner beside Settings tab in order to register SecuraLive® Ultimate Security.
- It will display the License registration page as shown below.
- Copy and paste the license number under username tab and password in password tab accordingly.
- Please proceed to fill up the rest of the information required and click on 'OK' to complete the registration process.
- Once registered it will display the message as “your License has been activated”.

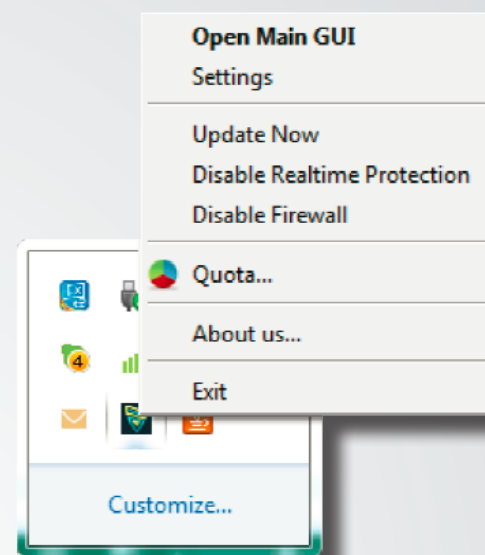
Restart the system after installing “SecuraLive® Ultimate Security in order to get the registry updated and work fine without any issues.



The screenshot displays the SecuraLive Ultimate Security software interface. On the left, a sidebar contains navigation options: ANTIVIRUS (Protection, Scan, Update, USB Guard), WEB PROTECTION (URL Categorization, Time Restrictions, Keywords), FIREWALL (Application Rules, Application Blocker, Bandwidth Monitor), and LOGS (Logs, Quarantine). The main window shows a 'License Registration' dialog box with the following fields: Username, Password, First Name, Last Name, Company (optional), Phone Number (optional), Email Address, and Country (a dropdown menu currently showing 'Afghanistan'). There is also a 'Note (optional)' text area and a checkbox for 'I would like to receive product news and special offers'. The dialog box has 'OK' and 'Cancel' buttons at the bottom right. In the background, the 'Register Now' button is visible in the top right corner of the application window.

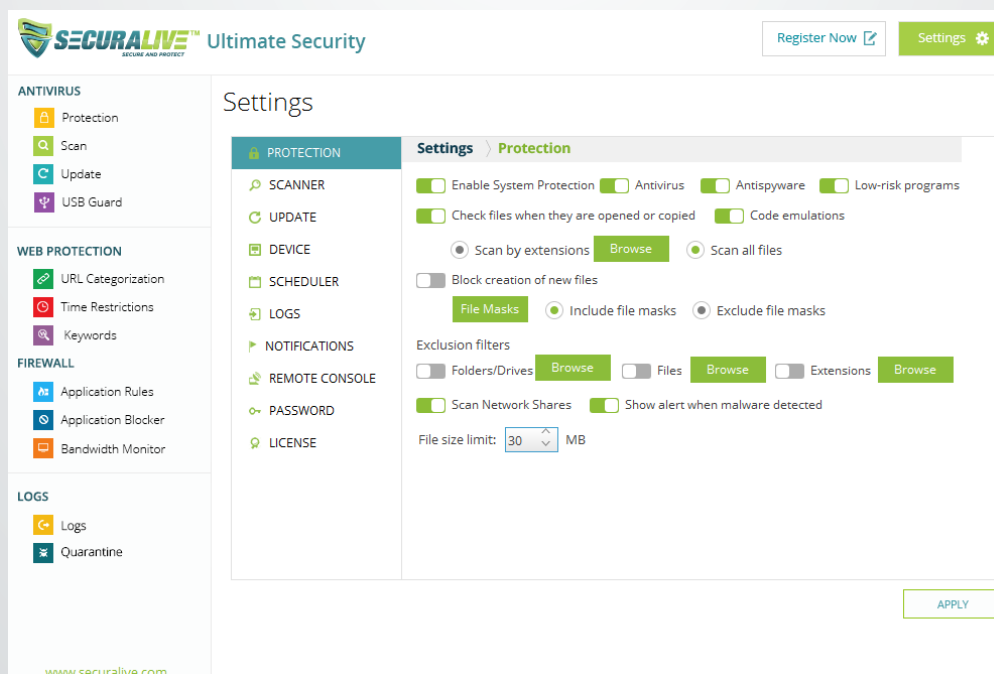
WORKING WITH SECURALIVE® ULTIMATE SECURITY

- After installation a SecuraLive® Ultimate Security shortcut icon will appear in your taskbar. Click on the icon to see the details of Ultimate Security.
- If you right click on the system tray icon it will display options to view the Main GUI, Settings, Update Now, Real-time protection, Firewall, Quota, About us and Exit options as shown.



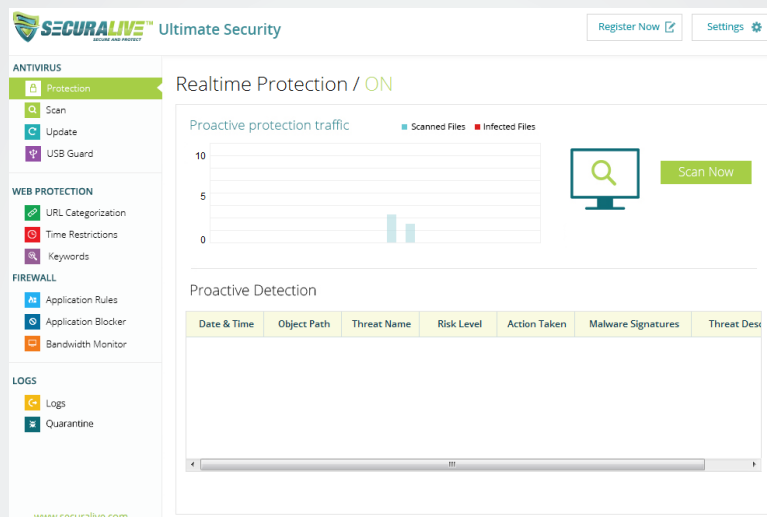
SECURALIVE ULTIMATE SECURITY OVERVIEW

- The SecuraLive Ultimate Security overview screen contains different options as shown below.
- Clicking on a screen will take you to that particular screen options.



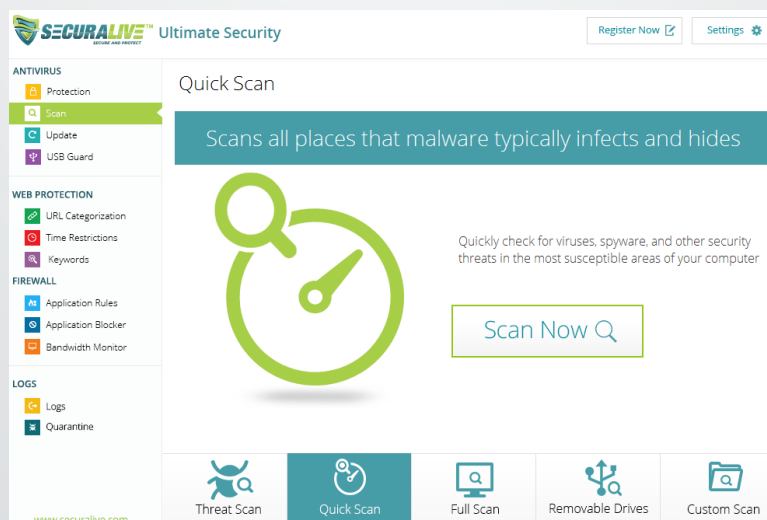
PROTECTION

- The protection tab shows whether Real-Time Protection is turned On/Off.
- It also displays the proactive Detection info at the bottom.



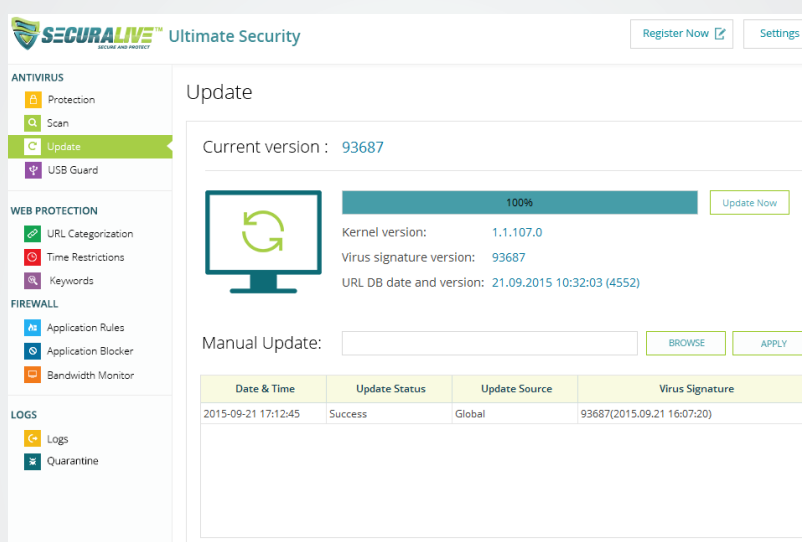
SCAN

- Please choose the appropriate “Scan” type from Threat Scan, Quick Scan, Full Scan, Removable Drives, and Custom Scan.
- Then click on “Scan Now”.
- You can also scan the files by right clicking on the file which gives you many options.



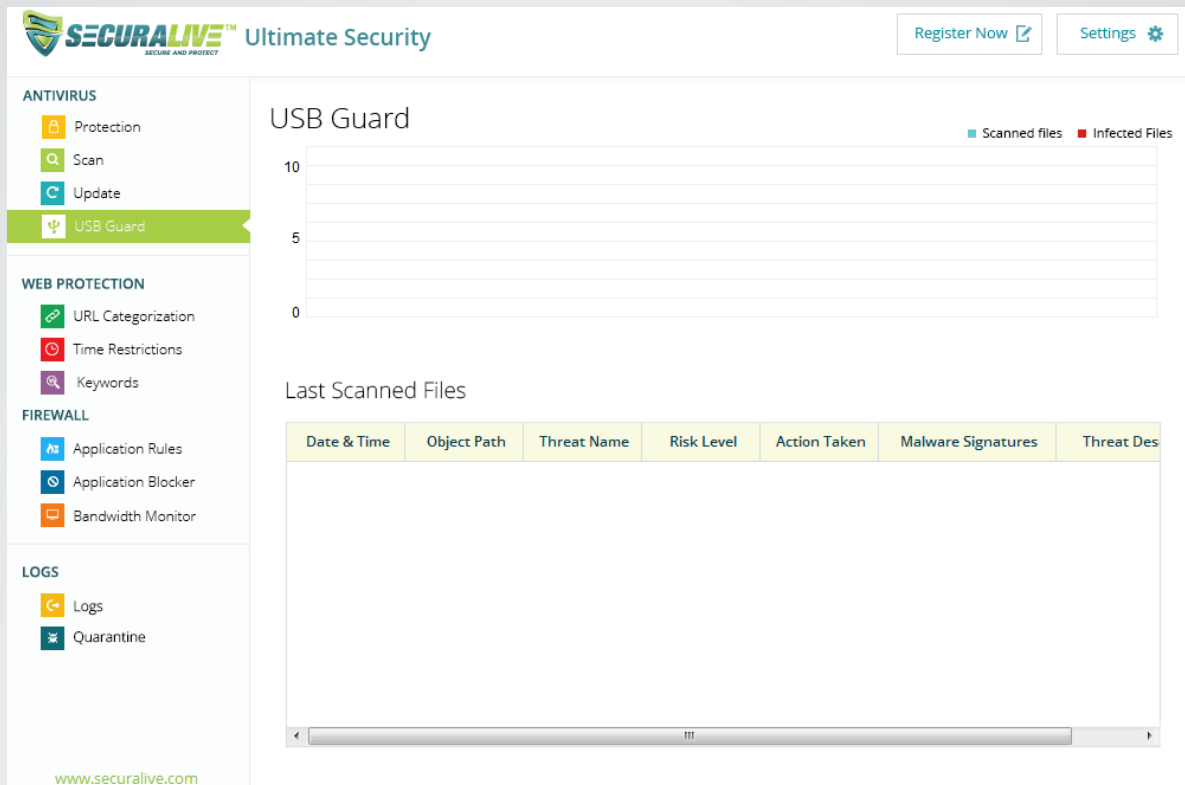
UPDATE

- Please click on “Update Now” for automatic updates from the server.
- You can also update SecuraLive® Ultimate Security manually by downloading the offline update file from here: <http://www.securalive.com/definitions>
- Once you have downloaded the file, Click on the “Browse” Option and find the file location to update and click on apply.



USB GUARD

- This will show the recent threat detection information and action taken. This includes USB detection as well as system threat detection information.



Steps to clear cookies from the browser before enabling any Category:

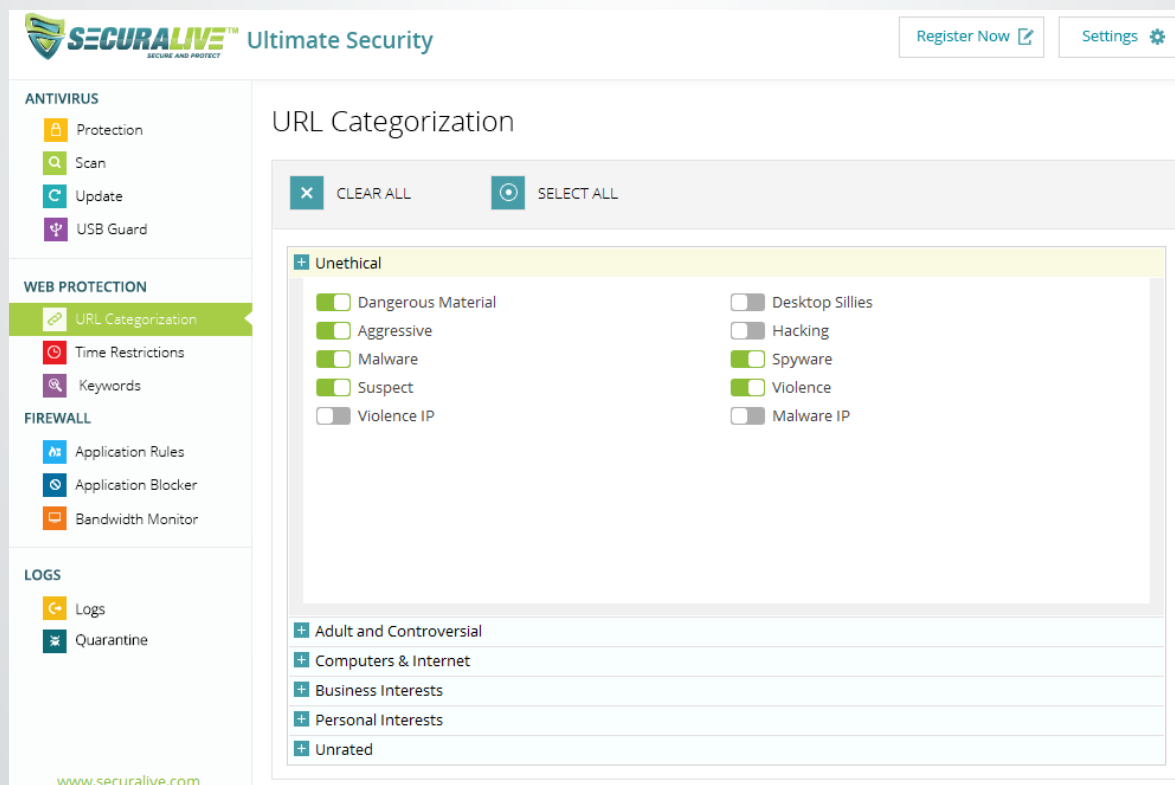
Please Note:

You are required to clear your Internet cookies, cache and other temporary files in your Internet browsers before enabling any Web Protection category. Failing to do so may result in websites being unblocked. You may follow below steps to clear the temporary files and other files as stated above.

- Open the browser i.e. Google Chrome.
- Click the menu bar on right hand side of the top corner.
- Scroll down to “History and recent tabs” and then click on History.
- It displays the browser’s history, click on “clear browsing data”.
- Select the required options as applicable and click on clear browsing data to delete the history.

CATEGORY WISE BLOCKING & PROTECTION

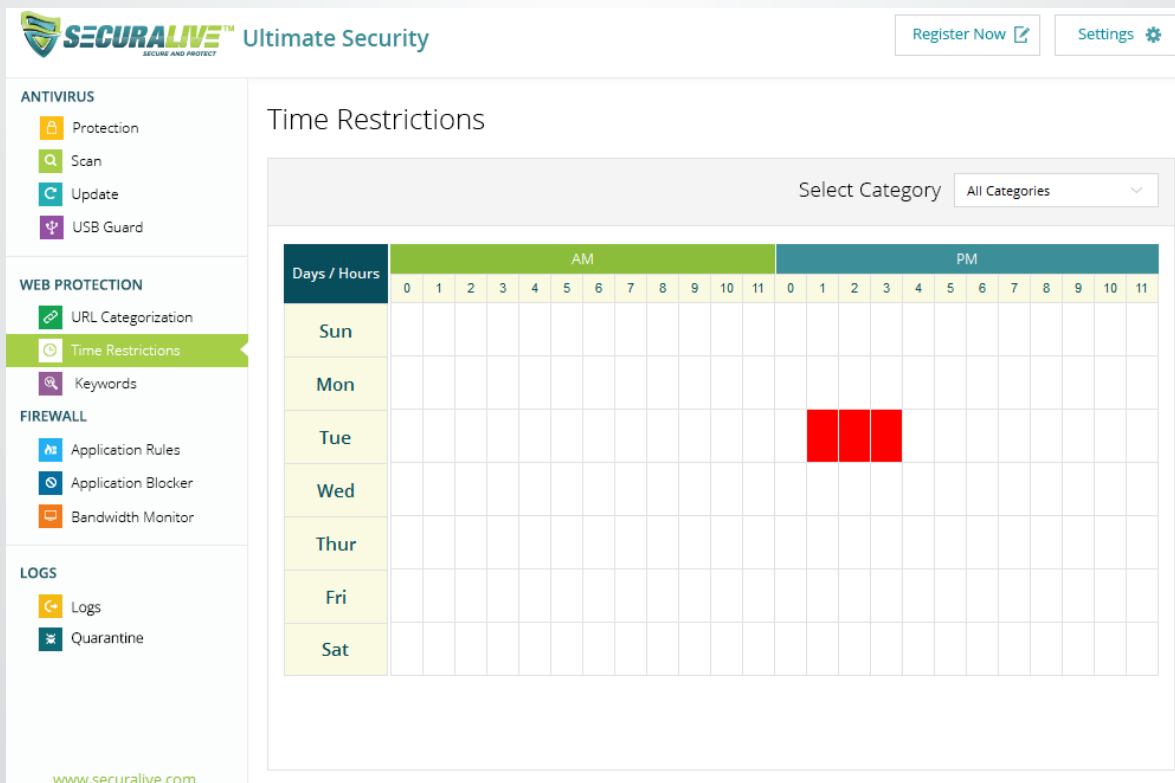
- You can configure the SecuraLive® URL categorization from the application.
- In the application based URL categorization, each row represents one feature. You simply have to check or uncheck checkboxes to enable or disable the features under the Categories section.
- When a check box is checked, then that particular feature is enabled.
- This feature ensures Web applications are used exactly as intended in organizations. It protects against the manipulation of Web environment for malicious intentions and provides an added level of security by the application infrastructure. It has a strong defense against known and emerging hacking attacks and has optimal predefined security rules for instant protection.



TIME RESTRICTION FEATURES

SecuraLive® Time Restriction is used to restrict web access according to daily time schedule and can be customised.

- Please click on “Time Restrictions” on the left-hand column menu.
- Please Select all categories or customise it and highlight a time to block, during which you wish to deny web access. Once you have selected the time (click and drag the mouse), a menu will pop up to block or allow that time.
- Press the “Save” button.
- Repeat until the Time Restrictions fit your needs.
- You can also allow a Time Selection instead of denying it.



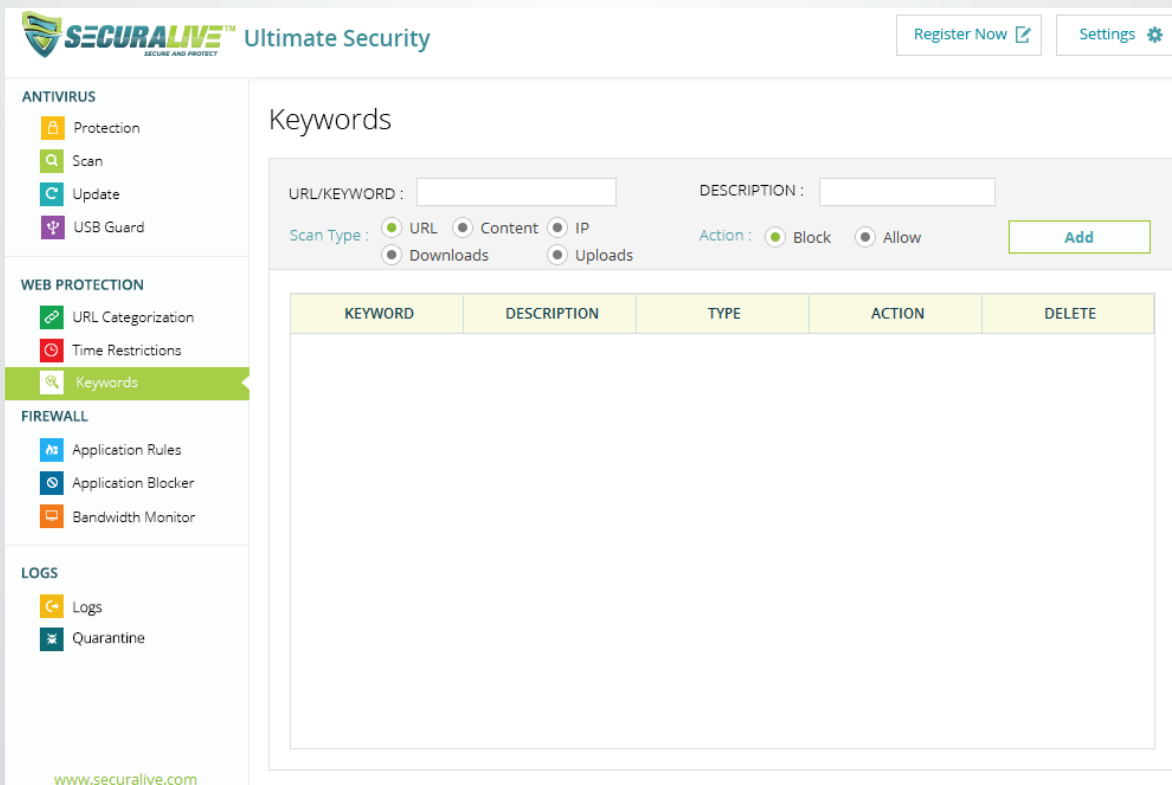
The screenshot shows the SecuraLive Ultimate Security web interface. On the left is a sidebar menu with categories: ANTIVIRUS, WEB PROTECTION, FIREWALL, and LOGS. The 'Time Restrictions' option under WEB PROTECTION is highlighted. The main content area is titled 'Time Restrictions' and features a 'Select Category' dropdown set to 'All Categories'. Below this is a grid for setting restrictions by day and hour.

Days / Hours	AM												PM											
	0	1	2	3	4	5	6	7	8	9	10	11	0	1	2	3	4	5	6	7	8	9	10	11
Sun																								
Mon																								
Tue																								
Wed																								
Thur																								
Fri																								
Sat																								

In the screenshot, three red squares are visible in the PM column for Tuesday, specifically at hours 1, 2, and 3, indicating that web access is restricted during this time.

KEYWORD BLOCKING

- Enter a keyword or domain in the Keyword/URL box, fill in the description box and select the match on options, then click “Add”.
- Some examples of keyword application are: If the keyword “Dating” is specified, the URL <http://www.xxx.com/dating.html> is blocked. If the keyword “.com” is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
- To delete a keyword or domain, select it from the list and click “Delete Keyword”.



The screenshot shows the SecuraLive Ultimate Security web interface. On the left is a sidebar with navigation links: ANTIVIRUS (Protection, Scan, Update, USB Guard), WEB PROTECTION (URL Categorization, Time Restrictions, Keywords), FIREWALL (Application Rules, Application Blocker, Bandwidth Monitor), and LOGS (Logs, Quarantine). The 'Keywords' link under WEB PROTECTION is highlighted. The main content area is titled 'Keywords' and contains a form for adding new keywords. The form has two input fields: 'URL/KEYWORD' and 'DESCRIPTION'. Below these are radio buttons for 'Scan Type' (URL, Content, IP, Downloads, Uploads) and 'Action' (Block, Allow). An 'Add' button is to the right. Below the form is a table with the following columns: KEYWORD, DESCRIPTION, TYPE, ACTION, and DELETE. The table is currently empty.

Keywords

URL/KEYWORD : DESCRIPTION :

Scan Type : ☒ URL ☐ Content ☐ IP ☐ Downloads ☐ Uploads

Action : ☒ Block ☐ Allow

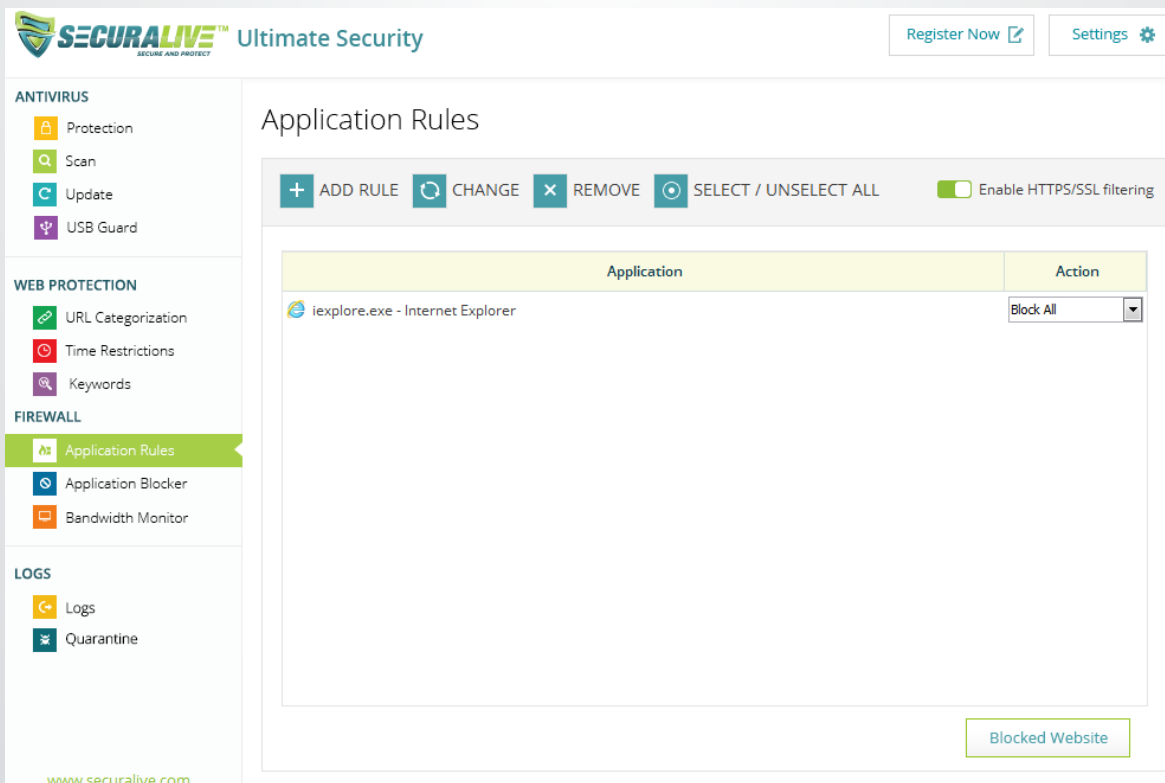
KEYWORD	DESCRIPTION	TYPE	ACTION	DELETE
---------	-------------	------	--------	--------

www.securalive.com

APPLICATION RULES

SecuraLive[®] Application Rules is used to block/restrict TCP/IP, UDP traffic based Internet protocols. It will show as the application is loading/accessing but will restrict and display the results.

- Please click on “Application Rules” on the left-hand column menu under Firewall.
- Please Enable HTTPS/SSL filtering button and click on ADD RULES.
- Select the application from the location and click open. E.g.: Chrome/IE/Firefox
- Select the option under custom rule as needed and click on apply.

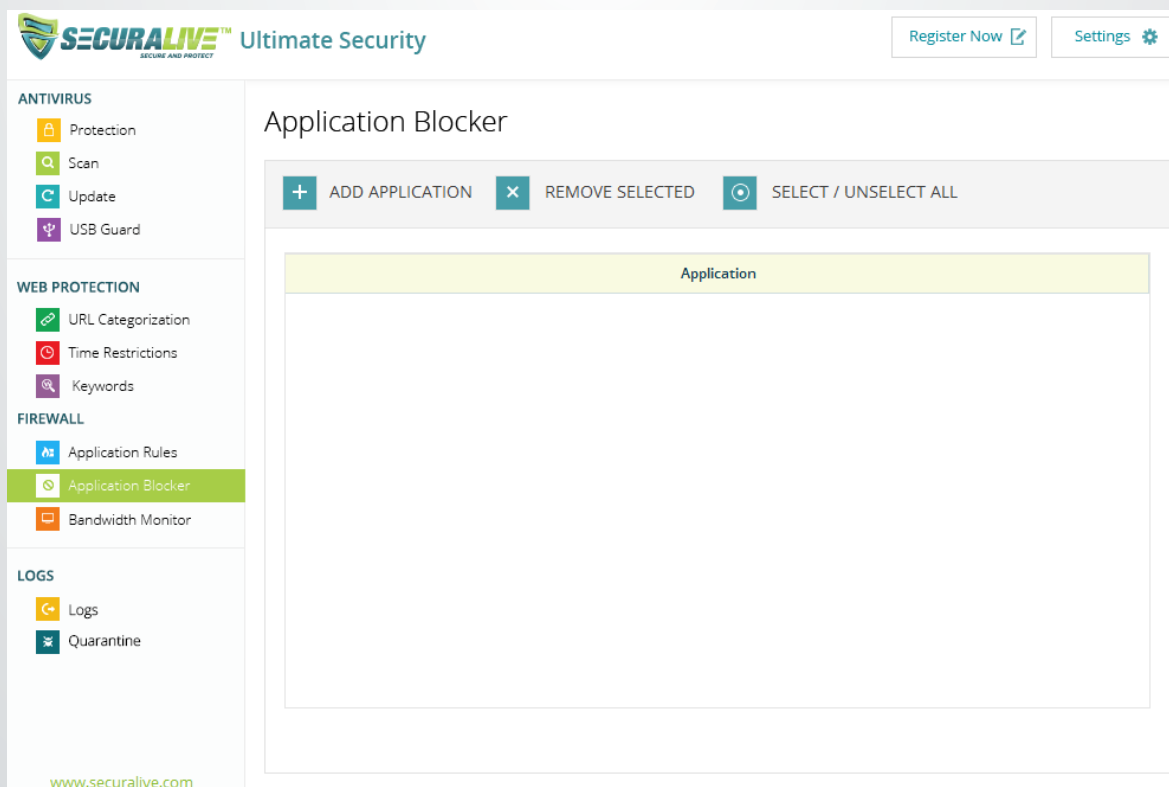


The screenshot shows the SecuraLive Ultimate Security interface. On the left is a sidebar menu with categories: ANTIVIRUS (Protection, Scan, Update, USB Guard), WEB PROTECTION (URL Categorization, Time Restrictions, Keywords), FIREWALL (Application Rules, Application Blocker, Bandwidth Monitor), and LOGS (Logs, Quarantine). The 'Application Rules' option under Firewall is selected. The main panel is titled 'Application Rules' and contains a toolbar with buttons: + ADD RULE, ↻ CHANGE, ✕ REMOVE, and ⏮ SELECT / UNSELECT ALL. To the right of the toolbar is a checkbox for 'Enable HTTPS/SSL filtering'. Below the toolbar is a table with two columns: 'Application' and 'Action'. The table contains one entry: 'iexplore.exe - Internet Explorer' with a dropdown menu set to 'Block All'. At the bottom right of the table area is a button labeled 'Blocked Website'. The top right of the interface has 'Register Now' and 'Settings' links.

APPLICATION BLOCKER

SecuraLive[®] Application Blocker is used to block/restrict application from being installed or executed.

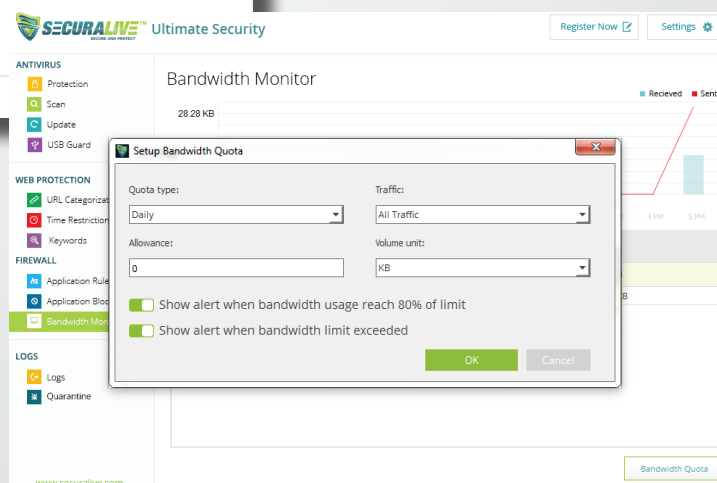
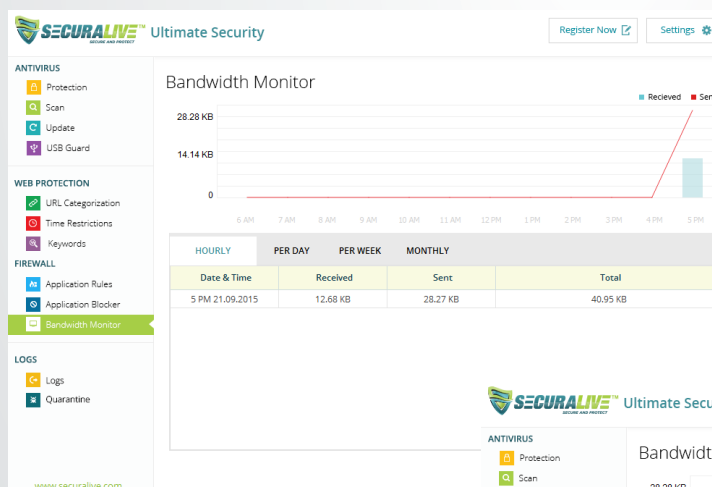
- Please click on “Application Blocker” on the left-hand column menu under Firewall.
- Please click on Add Application and select the .exe application from the location and click open e.g. skype.exe
- Once the application has been added to blocking list, the user will not be able to install or execute the particular application and it will display a message on the right side tray menu as “Application is blocked”



BANDWIDTH MONITOR

SecuraLive® Bandwidth Monitor is used to check the bandwidth or Internet usage on a particular system on a day to day basis. It displays the data received or sent in hourly, per day, per week and monthly basis. Bandwidth quota is used to allow or restrict the usage of Internet. We can set the usage limit in KB's, MB's and GB's.

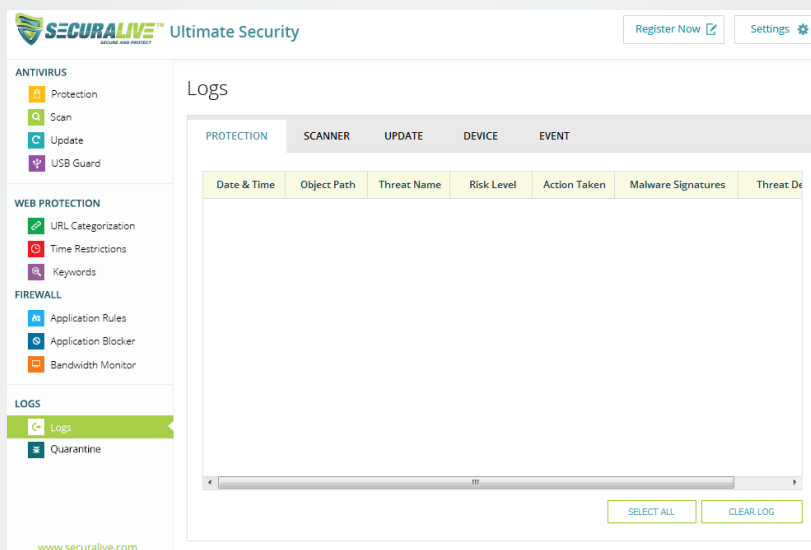
- Please click on “Bandwidth Monitor” on the left-hand column menu under Firewall.
- Then click on Bandwidth Quota option on the bottom of the Window.
- Specify the allowance and volume unit to restrict the Internet usage.
- Switch on the Alert option for the display message.
- When the user tries to access the Internet after the specified limit, it will display a message accordingly on the right side in tray menu.



LOGS

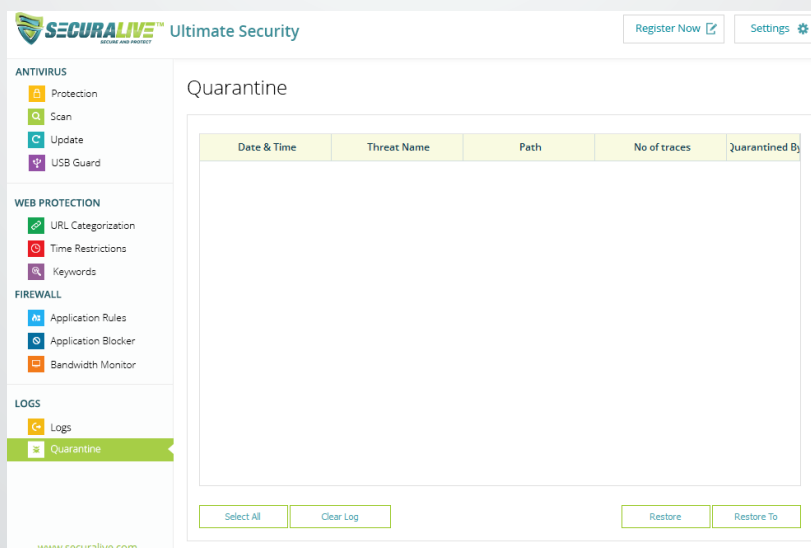
The “Logs” tab shows all the logs regarding the Ultimate Security functionality.

- By clicking on each of the 5 tabs as below, you can check out the logs of each tab (“Protection”, “Scanner”, “Update”, “Device”, and “Event”).



QUARANTINE

The “Quarantine” tab displays the list of quarantined files in your system such as trap doors, logic bombs, worms etc.



SETTINGS

PROTECTION

Click on the “Settings” tab which has the wheel symbol on the top right hand corner of the GUI. In the “Protection” tab you are able to enable or disable the scanning options for the Folders/Drives.

- You can include or exclude the scanning options of the external devices when it is connected to the system.
- If you make any changes, then click on “APPLY”.

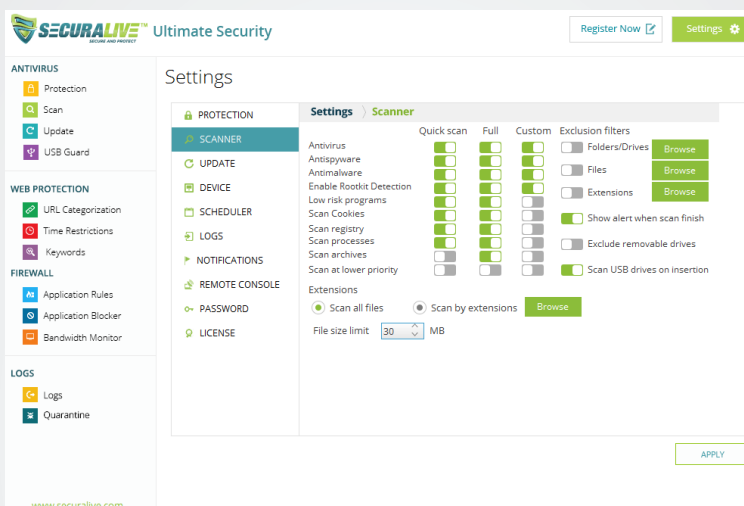
For e.g.: if you disable code emulations, it results in the protection status of code emulations at risk.



SCANNER

In the “Scanner” tab, there are lot more options on scanning.

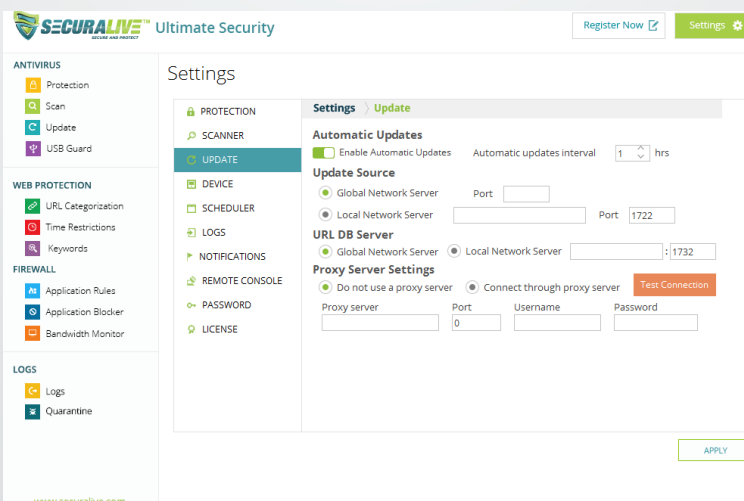
- You can include the extensions to scan automatically when the program is running.
- If you make any changes, then click on “APPLY”.



UPDATE

In the “Update” tab, you can enable or disable the automatic updates.

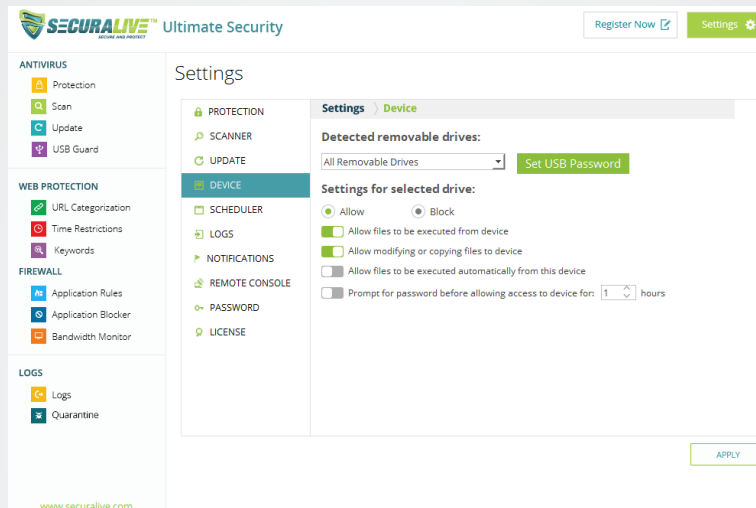
- You can set the Update source i.e. global or local.
- You can set whether to use the proxy server or not.
- If you make any changes, then click on “APPLY”.



DEVICE

In the “Device” tab, you can disable or enable the external devices.

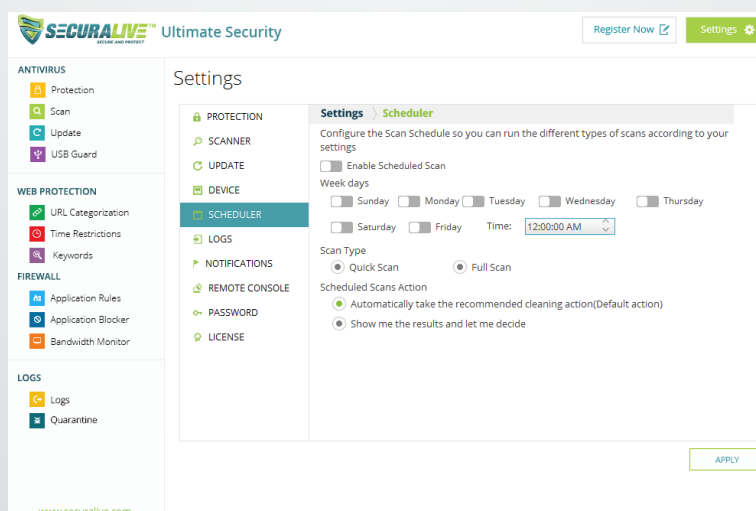
- You can give permissions to the external devices.
- You can allow/block devices based on your needs.
- If you make any changes, then click on “APPLY”



SCHEDULER

In the “Scheduler” tab you can schedule when system scanning needs to be carried out. Here you can change the default scanning (full or custom scan).

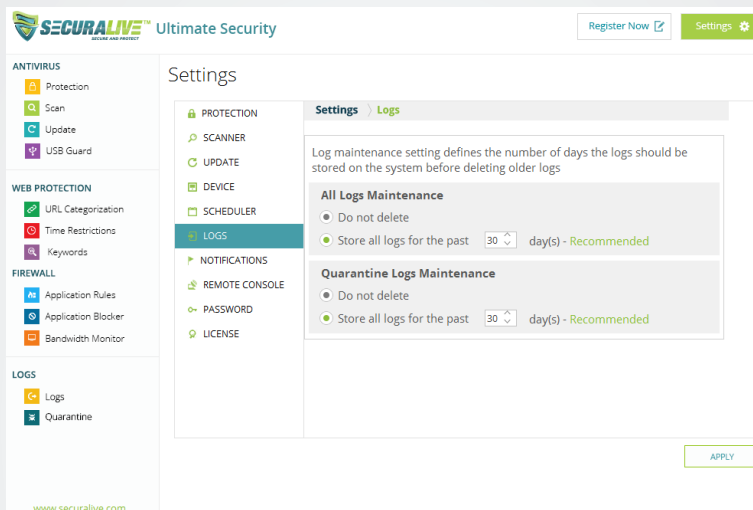
- If you want to scan your system every day, then select all the days.
- If you make any changes, then click on “APPLY”.



LOGS

In the “Logs” tab you can change the settings regarding the logs.

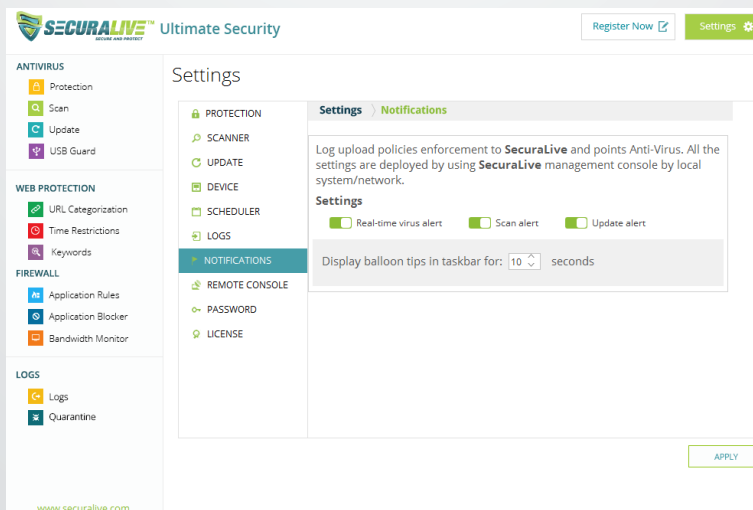
- If you want to delete the logs on/before 30 days you can set the option to 30 days. We suggest you to keep the recommended settings.
- If you make any changes, then click on “APPLY”.



NOTIFICATION

The “Notification” tab will give alert messages to the user.

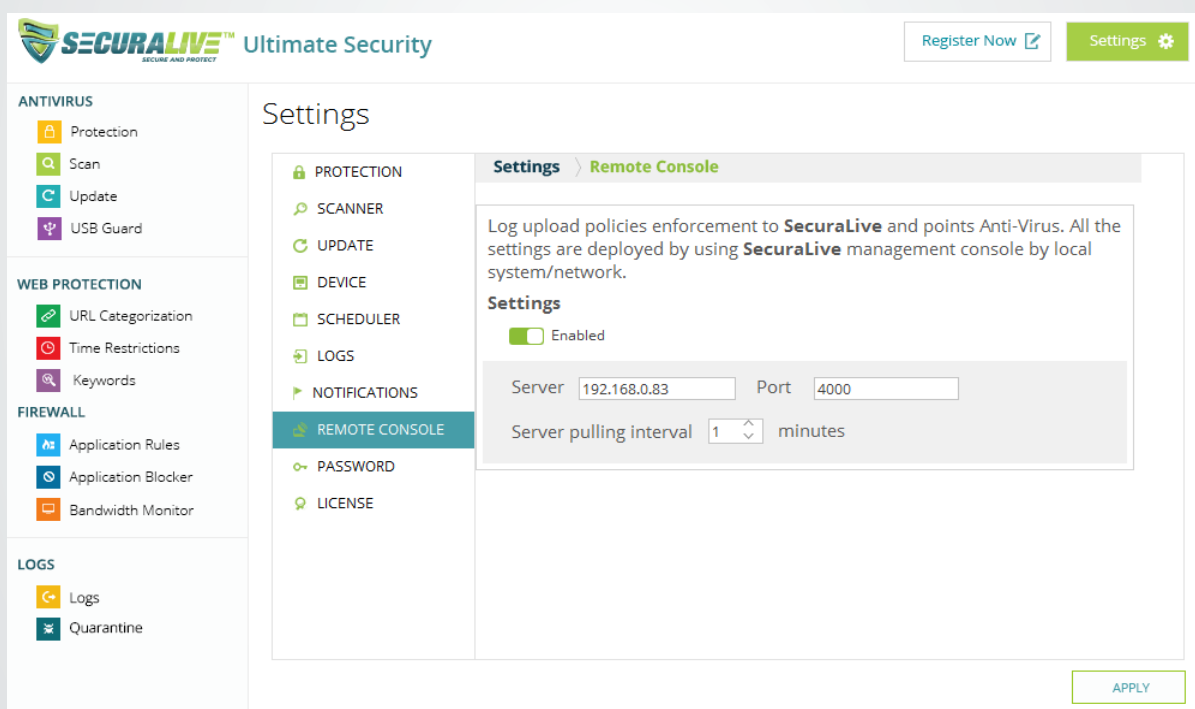
- If any malicious program enters the system then it will give an alert message to the user.
- If you make any changes, then click on “APPLY”.



REMOTE CONSOLE

If your system is on a network and there is a server then the “Remote Console” tab will come into the picture.

- If you have set a server IP and the port number then it will be connected to that particular network.
- If you make any changes, then click on “APPLY”.



The screenshot shows the SecuraLive Ultimate Security management console. The left sidebar contains navigation links for ANTIVIRUS, WEB PROTECTION, FIREWALL, and LOGS. The main content area is titled 'Settings' and has a sub-tab 'Remote Console'. The 'Remote Console' section includes a description: 'Log upload policies enforcement to SecuraLive and points Anti-Virus. All the settings are deployed by using SecuraLive management console by local system/network.' Below this, there is a 'Settings' box with an 'Enabled' checkbox, a 'Server' field with the value '192.168.0.83', a 'Port' field with the value '4000', and a 'Server pulling interval' dropdown set to '1' minutes. An 'APPLY' button is located at the bottom right of the settings area.

SECURALIVE[™] Ultimate Security [Register Now](#) [Settings](#)

ANTIVIRUS

- Protection
- Scan
- Update
- USB Guard

WEB PROTECTION

- URL Categorization
- Time Restrictions
- Keywords

FIREWALL

- Application Rules
- Application Blocker
- Bandwidth Monitor

LOGS

- Logs
- Quarantine

Settings

Settings > Remote Console

Log upload policies enforcement to **SecuraLive** and points Anti-Virus. All the settings are deployed by using **SecuraLive** management console by local system/network.

Settings

☒ Enabled

Server Port

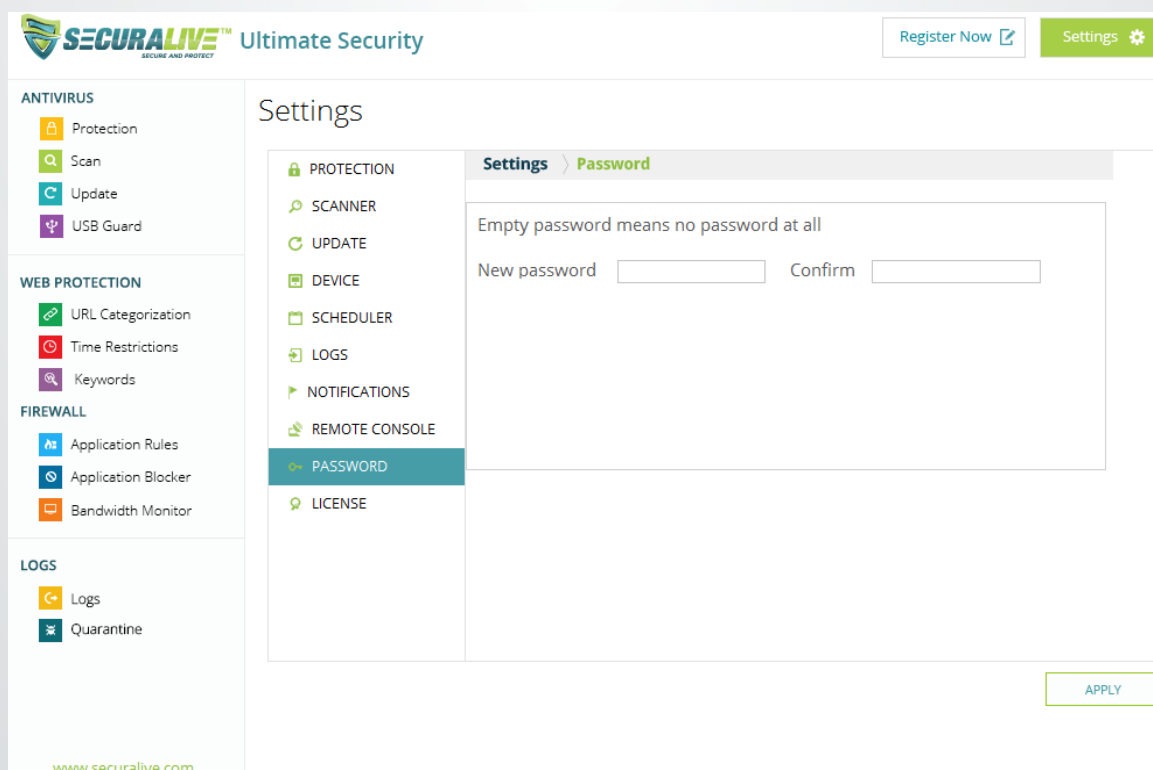
Server pulling interval minutes

APPLY

PASSWORD

The “Password” tab, is used to set the password for the GUI.

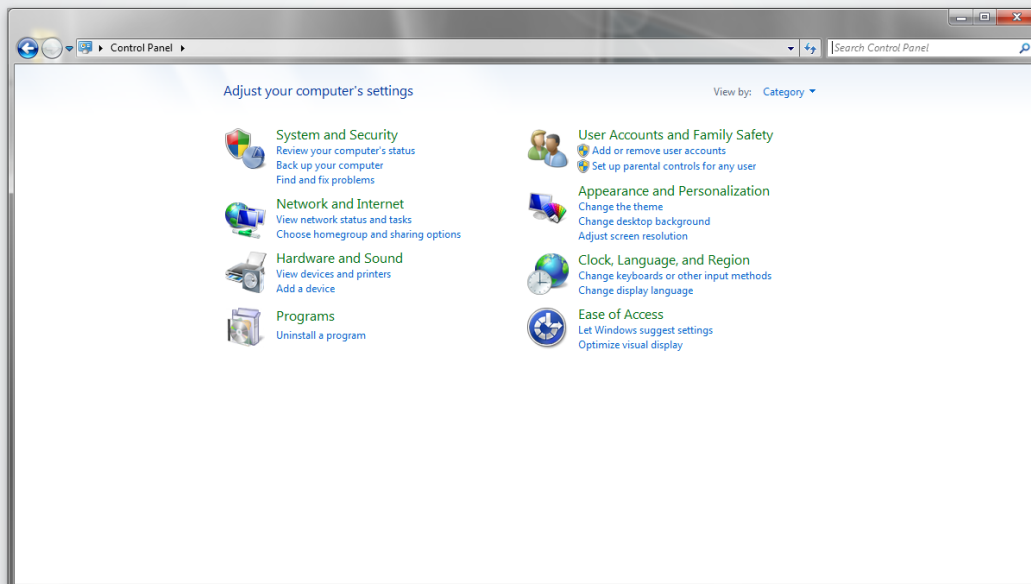
- If you set the password then no one can change your settings in SecuraLive® Ultimate Security for various options like URL Categorization, Time Restriction, Keywords, Application Rules, Application Blocker, and Bandwidth Monitor.
- Anyone who is trying to access or login into SecuraLive® Ultimate Security will prompt the person to put in the password to open, without which he/she cannot change any settings in it.
- Only the Administrator will be able to access and change the settings in SecuraLive® Ultimate Security.
- The Default password is empty. If you make any changes, then click on “APPLY”.



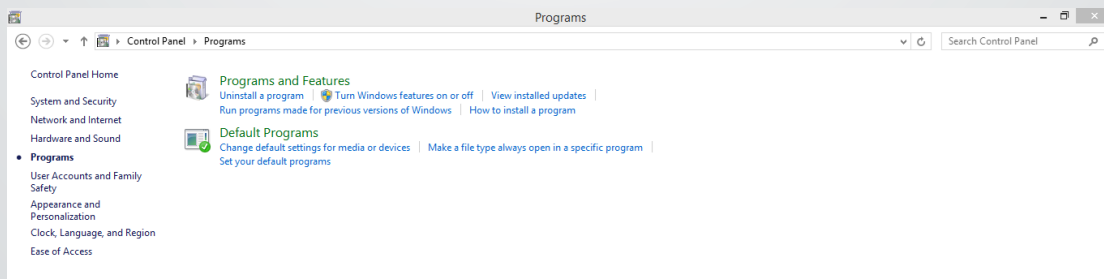
Uninstalling SecuraLive® ULTIMATE SECURITY

To uninstall the SecuraLive® Ultimate Security, click on the “Start Menu” button on the taskbar then go to “Control Panel”.

- In control Panel screen click on Programs menu option



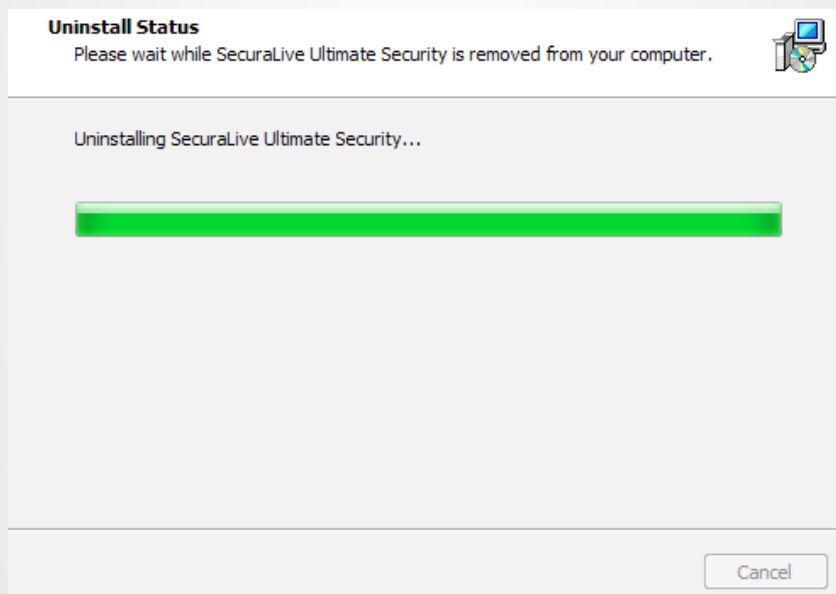
- Please click on “Programs & Features” and it will direct you to “Uninstall” a Program.



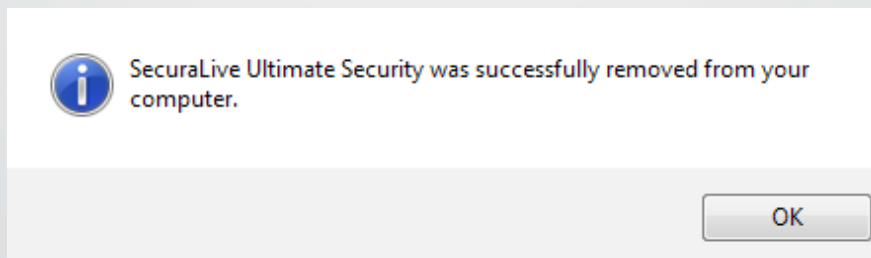
- This will navigate you to a list of the system programs that you have installed. Select “SecuraLive® Ultimate Security Version 10.0.1.5” program and right click. It will then show you the option to uninstall the program as shown in the image.
- Click on “Uninstall” and follow the process to uninstall.

SecuraLive Ultimate Security version 10.0.1.5		15-09-2015	286 MB	10.0.1.5
Skype™ 7.8	Uninstall	Technologies S.A.	24-08-2015	71.1 MB 7.8.102

- Then the process of un-installation will start and continue until the whole green colored bar is filled.



- A message will be displayed after successful uninstallation as below.



Technical Support:

For Technical Support on SecuraLive® Products, please visit
www.securalive.com.

Technical Support is provided either via Live webchat or by submitting a
Support ticket on our website.

(c) 2014 - 2015 SecuraLive®, SecuraLive® is a Registered Trademark of PCRange Pty Ltd.
No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical,
including photocopying, recording, or by any information storage and retrieval system, without written
permission from SecuraLive®.

Sales: sales@securalive.com
Support: support@securalive.com
Website: www.securalive.com